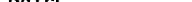


Attorney Docket 60323/462-96-004
CERTIFICATE OF MAILING BY "EXPRESS MAIL"

**"Express Mail Mailing Label Number
EH607069675US**

Date of Deposit May 22, 1997
I hereby certify that this paper or fee is
being deposited with the United States Postal
Service "Express Mail Post Office to
Addressee" Service under 37 CFR §1.10 on the
date indicated above and is addressed to the
Assistant Commissioner for Patents,
Washington, D.C. 20231.

ED PRICE
(Typed or printed name of person mailing)

(Signature of person mailing)

COPY PROTECTION FOR DATABASE UPDATES TRANSMITTED VIA THE INTERNET

CROSS REFERENCE TO RELATED APPLICATIONS

5

The present application is based upon and claims priority of U.S. Provisional Application No. 60/021,702, filed on July 12, 1996.

10

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a system for protecting the unauthorized use of software transmitted over a communication link and more particularly to a system in which the software is encrypted with a unique software key that only allows the software to be uploaded into a unit, such as global positioning system (GPS) unit, with a matching software key.

2. Description of the Prior Art

20 Global positioning systems are known to be used
in aircraft and other vehicles for navigation. Such GPS
systems not only provide the position of the aircraft or
vehicle but may also be integrated with topographical
and/or navigational data, such as terrain and airport
25 topographical data as well as highway maps stored in a

database, to provide an indication of the vehicle or aircraft relative to the topographical data or highway information. For example, as disclosed in U.S. Patent Application Serial No. 08/509,642 filed on July 31, 5 assigned to the same assignee of the present invention, the topographical data, such as the elevation of the highest obstacles within a predetermined region, are stored in a memory device aboard the aircraft. The GPS allows the topographical data to be displayed as a 10 function of the position of the aircraft.

Often times, the topographical and navigational data needs to be updated due to changing topography and highway information. Because of the relative ease in which software that is transmitted over the Internet can be duplicated, updates of the topographical data is known to be provided in a diskette or cartridge form and mailed to the customers. Typically, users of such integrated GPS systems must first determine if an update is available by checking with the database vendor. 15 Orders are typically placed by telephone. The update diskette or cartridge is then mailed to the customer. As such, from the time the order is placed, considerable time passes before the updated topographical data is actually received by the customer so it can be uploaded 20 into the customer's integrated GPS unit. The delay is even more acute for international customers for which the mailing time is considerably greater. 25

There are other problems associated with providing updated topographical and navigational data on diskettes or cartridges to a customer. For example, for 30 customers that have multiple integrated GPS units, the customer may choose to upload the updated data onto such multiple units even though the customer has only paid for the update for a single unit. The customer may also 35 transfer the update diskette or cartridge to another unauthorized user.

Sub
D1
N 62250-62679880

SUMMARY OF THE INVENTION

It is an object of the present invention to solve various problems in the prior art.

It is yet another object of the present invention to provide a system for preventing unauthorized use of a database or other software transmitted over a communication link, such as the Internet.

Briefly, the present invention relates to a system for transmitting a database or other software over a communication link, such as the Internet, which prevents unauthorized use. In order to prevent such unauthorized use, the customer's equipment, such as a GPS unit, is provided with a unique software key. The updated database is ordered over the communication link by providing the unique software key and may include electronic payment information. The database is encrypted, for example, as a function of the unique software key and transmitted over the communication link in encrypted form along with an upload program. The upload program only allows the encrypted database to be uploaded into a unit with a matching software key. As such, the system allows updated databases to be transmitted rather quickly and easily over a communication link while preventing unauthorized use.

DESCRIPTION OF THE DRAWINGS

These and other objects of the present invention will be readily understood with reference to the following specification and attached drawings wherein:

FIG. 1 is a graphical illustration of an exemplary Internet page layout in accordance with the present invention:

35 FIG. 2 is a simplified representation of a dialog box which may form a part of one of the Web pages

for user information, such as the unique software key, in accordance with the present invention;

FIG. 3 is a simplified view of a personal computer interfacing with an Internet server in order to provide user information;

FIG. 4 is similar to FIG. 2 illustrating the process of downloading the software from the Internet to a user's personal computer;

FIG. 5 is a simplified graphical representation illustrating the uploading of the software from the Internet being transferred between a personal computer and a product, such as an integrated global positioning system (GPS) unit;

FIG. 6 is a block diagram illustrating the data flow and the organization of the software on the Internet server in accordance with the present invention;

FIG. 7 is a simplified flowchart illustrating a portion of the system in accordance with the present invention for ordering software over the Internet;

FIG. 8 is a graphical representation of a dialog box for user payment information which may form a portion of one of the Web pages illustrated in FIG. 1 in accordance with the present invention;

FIG. 9 is a graphical illustration of a dialog box for enabling users to provide information regarding the requested software as well as a unique software key which may form a portion of one of the Web pages illustrated in FIG. 1 in accordance with the present invention;

FIG. 10 is a graphical illustration of a dialog box for the user's desired payment method which may form a portion of one of the Web pages illustrated in FIG. 1 in accordance with the present invention;

FIG. 11 is a graphical illustration of a confirmation page which may form a portion of one of the

08854980 08854981 08854982 08854983

Web pages illustrated in FIG. 1 which enables the user to download software over the Internet in accordance with the present invention;

5 FIG. 12 is a flowchart of the system in accordance with the present invention which provides copy protection for software transferred over the Internet in accordance with the present invention;

10 FIG. 13 is a flowchart of the software at the server for encrypting the software to be transferred over the Internet in accordance with the present invention; and

15 FIG. 14 is a flowchart of the decryption process for uploading software transferred over the Internet to a customer's unit, such as an integrated global positioning system (GPS) unit.

DETAILED DESCRIPTION

The present invention relates to a system for preventing unauthorized use of a database or other 20 software transmitted over a communication link, such as the Internet, for use in particular electronic equipment, such as a global position system (GPS) unit. As mentioned above, such systems utilize topographical data for various regions of the world in order to 25 display the topographical data as a function of the position of the aircraft. Heretofore such GPS units have been sold with topographical and/or navigational data stored in a database on cartridges or diskettes. Updated databases are known to be shipped through the 30 mail. Such a process takes a relatively long period of time. The system in accordance with the present invention allows the database update to be transmitted over communication links, such as the Internet quickly and easily while virtually eliminating unauthorized use 35 of the database information. More particularly, each GPS unit is provided with a unique software key. The

20250000000000000000000000000000

PK
*ROM
or
cartridge
memory
of key*

unique key is an 8 digit hexadecimal number, which may be embedded in a read only memory (ROM) within the GPS unit or stored within a removable cartridge at the factory prior to a GPS unit being shipped to the customer. The user uses the unique software key to order update software, such as an update database for the GPS unit, over the communication link and upload the database into a GPS unit with a matching software key, for example as illustrated in FIGS. 3, 4 and 5. For example, the user simply connects to the GPS database or other software vendor's home page on the WorldWide Web. After providing the unique software key number as well as the desired payment method, the database or other software is encrypted as a function of the unique software key at the Internet server, for example. The encrypted software is transmitted to the user over the Internet along with a decryption program which only allows the software to be uploaded into a GPS unit having a matching key. Since the updated database is encrypted as a function of the unique software key, any attempts to upload the software into a unit not matching the unique software key will be futile. Although multiple copies of the encrypted database can be made, the system in accordance with the present invention prevents these encrypted copies from being uploaded into multiple GPS units.

The present invention is suitable for updating the topographical information stored in databases for use with various integrated GPS systems, such as, KLX 30 100 GPS/COMM, KLN 98/KLN 89B GPS, KLN 90B GPS and KLN 900 GPS, available from AlliedSignal, Incorporated. Although the system in accordance with the present invention is described and illustrated in terms of transferring updated database information for an integrated GPS over the Internet, the principles of the present invention are clearly applicable to protecting

virtually any type of software transmitted over virtually any communication link; wired or wireless.

It is also to be understood that the principles of the present invention are also applicable to other forms of electronic transfer that do not involve the Internet and may be implemented for transferring software over virtually any communication link, such as a modem and even a wireless link. Moreover, as will be discussed in more detail below, a personal computer is used to access the Internet server, for example, which contains the software to be transferred as illustrated in FIGS. 3 and 4. The desired software is then encrypted and transferred along with a decryption program back to the personal computer, which, in turn, is used to transfer and decrypt the software into a separate electronic unit, such as an integrated GPS unit. However, it should also be understood that the principles of the present invention are also applicable to systems in which the desired software is also transmitted from a remote communication node, such as an Internet server, directly to the unit, such as the integrated GPS unit itself.

Referring to FIG. 1, an exemplary Web page layout is illustrated. The exemplary Web page layout includes a home page 22. The home page 22 is provided with one or more hyperlinks to provide access to the succeeding Web pages. As shown, the home page 22, for example, as illustrated in FIG. 8, may be provided with a hyperlink to a database selection page 24 (FIG. 9). The database selection page 24 enables a user to select the specific database. As mentioned above, depending upon the type of integrated GPS unit, various update databases are available for transfer over the Internet. After the particular database is selected from the database selection page 24, a hyperlink may be provided to a method of payment Web page 26 with hyperlinks to a

credit card Web page 28 (FIG. 10) and a user password Web page 30. It is to be understood that the payment option is merely optional. The credit card Web page 28 and the user password Web page 30 allow alternate payment methods for the user in systems which include electronic payment. The credit card Web page 28 requires the user's credit card information as well as the unique software key (FIG. 2). Alternatively, the system allows for the customer to contact the software supplier ahead of time and establish an account. In this situation the user merely enters a password for the account as well as the unique software key for the unit. The credit card Web page 28 and the password Web page 30 are provided with hyperlinks to a confirmation page 32 (FIG. 11). The confirmation page 32 is merely exemplary and is not required for practice of the invention. The confirmation page 32 confirms the user's selection for the particular database as well as the method of electronic payment. If the user enters a confirmation, a hyperlink may be provided on the confirmation page 32 to initiate downloading of the updated software, which is linked to a message page 34 which indicates downloading in progress.

FIGS. 3 through 7 illustrate the present invention. As shown, user information is transferred over the Internet to one or more Internet servers 36 by way of a personal computer which may be an IBM compatible personal computer or other personal computer suitable for connection to the Internet. The software 30 is encrypted and then transferred from one or more Internet servers 36 back to the personal computer 38 along with a decryption and upload program. The upload program enables the encrypted database to be uploaded into a product with a matching software key, such as an integrated GPS unit 40.

A Sub D2

The software layout for the system is illustrated in FIG. 6 and includes a user database 40, a master "nav" database 42 and an upload program ⁴⁴, identified as NETLOAD.EXE. The user information for example, regarding account and password information, etc. is maintained in the user database 40, accessible by the server 36. The topographical information is stored in the master "nav" database file 42, also accessible by the server 36. Once the user provides the unique software key as well as the desired payment method, a copy of the topographical and/or navigation data from a master "nav" file 42 is encrypted as a function of the unique software key, provided by the user and stored in a "keyed DB file" 44. The keyed DB file 44 is then compressed into a zip file 46 and transferred to the user by way of the Internet along with the decryption or upload file ⁴⁴, identified as NETLOAD.EXE. The decryption file ⁴⁴ enables the zip file containing the encrypted database to be uploaded into a product 40 as long as the software key of the product matches the software key to which the database was encrypted. If the software key matches the unique key within the product, the database is decrypted and uploaded into the product.

A simplified flowchart for the system in accordance with the present invention is illustrated in FIG. 7. Initially, the user connects to the database vendor's home page in step 48. Once connected to the database vendor's home page, the user selects a database from the available databases in step 50. Steps 52 and 54 provide for alternate payment methods. If a user wishes to avoid providing credit information over the Internet, the user can obtain a password and an account and become a registered user. Thus, the system checks whether the user is a registered user in step 52. If not, the system assumes the payment will be made by

00000000000000000000000000000000
262250-68678800

credit card in step 54. In both steps 52 and 54, the user also provides the unique software number that is used to encrypt the database as a function thereof. After the payment method and unique software key are entered, a confirmation page is generated in step 56, for downloading the software.

An overall flow chart is illustrated in FIG. 12. Initially, the unique software key, for example, the 8 digit unique software key unique to the GPS system, is read from the GPS unit 40 by the user and entered on the appropriate Web pages as discussed above. The software key may be printed somewhere on the GPS unit 40 to enable the user simply visually read the software key from the unit in step 58. In step 60, the user logs onto the Internet, chooses a database product and provides the unique software key for the GPS unit 40. The system encrypts the selected database as a function of the unique software key and stored into a keyed database file 44 (FIG. 6) in step 62. In order to conserve storage space, the keyed database file 44 may also be compressed in step 63 and transferred to the customer personal computer 38 in step 64 along with a decryption program 44, identified as NETLOAD.EXE. The keyed database file is then uploaded by the user to their GPS unit 40 (FIG. 5) with a matching software key in step 66.

The flowchart for the database encryption or keying is illustrated in FIG. 13. After the user logs onto the Internet, selects a database and provides the unique software key, the system checks in step 68 whether the desired database is a type KLN 90 database. As used herein the KLN 90 type databases relates to the type of processor within the GPS unit 40. In particular, KLN 90 type databases are formatted for use with Intel type processor chips, while the balance of the databases are formatted for use with Motorola type

00000000000000000000000000000000

processor chips. Due to the different byte storage methods between the two processor styles, the system checks in step 68 whether request is for a type KLN 90 database. If so, a temporary file is created in step 70 with the database key embedded into the original KLN 90 file from a master KLN 90 database file 72, a subset of the master "nav" DB files 42. If the request is for other than KLN 90 type database, the system proceeds directly to step 74. In step 74, starting with the first byte, the byte is encrypted as a function of the database key, for example by cyclic redundancy coding (CRC), as discussed below. After the first byte is coded with the database key, the key is updated for the next byte in step 76. The keyed or encrypted byte is written to an output file 82 for later transmission over the Internet to the user's personal computer 38 in step 78. This process is continued until all of the bytes in the database file have been keyed and written to the output file 82 as illustrated by step 80. After all of the bytes have been written to the output file 82, a footer tag with data from the original file, including checksums, file size, database type, the effective dates and the original database key are written to the output file 82 and sent to the user along with the upload file NETLOAD.EXE in step 82 as discussed above. If the software key in the GPS unit 40 matches the database key, the NETLOAD.EXE file decrypts and uploads the updated database into an integrated GPS unit 40.

FIG. 14 is a flowchart for the decryption program ⁴⁵ (NETLOAD.EXE) for uploading the encrypted database software to the GPS unit 40. As mentioned above, the encrypted database file 82 is provided with the encrypted data as well as a footer tag which includes the original software key, checksums, the file size, the database type as well as the effective dates for the database. In step 86, the footer tag is read

30

35

A
Sub 7
D3 7

Sub
D3

including the software key from the encrypted output file 82. As discussed in more detail below, the software key from the footer tag is used to decrypt the first byte of the database in step 88. After the first byte is decrypted, the key is updated for the next byte in step 90. After the new key is updated, a checksum is calculated to determine if there are any errors in the data in step 92. The process of steps 88-92 is repeated for each byte in the encrypted database file 82, as indicated by step 94. After all of the bytes in the output file 82 have been decrypted, the system checks in step 96 to determine whether the checksum for the decrypted file matches the original checksum included in the footer tag in the output file 82 in step 96. If there are any discrepancies in the checksum an error message is displayed in step 98. If the checksums match, the system communicates with the GPS unit 40 in step 98 and awaits for the GPS unit 40 to send an identification packet containing the GPS unit type as well as the software key. Once the software key and GPS unit type are received from the GPS unit 40, the system determines in step 100 whether the GPS unit type matches the database file requested. If not, an error message is displayed in step 102. Otherwise, the system proceeds to step 104 and ascertains whether the software key received from the GPS unit 40 matches the software key used to encrypt the database file and contained in the footer tag mentioned above. If not, an error message is displayed in step 106. Otherwise, the system proceeds to step 108 where the software key received from the GPS unit is used to decrypt the first byte in the output file 82. After the first byte is decrypted or unkeyed, the key is updated in step 110 for the next byte. The steps 108 and 110 are repeated until a sufficient number of bytes have been unkeyed for a full packet as indicated in step 112. Each time a packet is

Sub
D3

full, a packet of decrypted data is sent to the GPS unit 40 in step 114. As indicated in step 116, the process is repeated until all of the bytes in the encrypted database file have been processed.

Essentially the encryption process is based on cyclic redundancy code (CRC) table of 256 pseudo random numbers from 0 to 255, for example, as illustrated in TABLE 1.

TABLE 1

	CRC TABLE ENTRY	VALUE
10	0	0
	1	1996959894
	2	3993919788
	3	2567524794
15	...	
	...	3188396048
	...	
	...	
	141	2466906013
20	...	
	...	
	237	3736837829
	...	
25	255	

Initially, a seed CRC value is chosen, for example 13579246. The first byte in the database or source file is read and added to the seed value. For example, if the first byte in the database equates to the number 3, the new byte will be the CRC seed value (13579246) plus the byte read from the file Boolean ANDed with the hexadecimal number FF or 255. For example, adding the value of the source byte 3 to the seed value of 13579246 would equal the number 13579249.

Taking the number 13579249 and Boolean ANDing it with the hexadecimal number 255 yields the number 241. Therefore, the new byte written to the file as shown in TABLE 2 below will be 241.

5

TABLE 2

10

ORIGINAL DATA FILE	NEW DATA FILE	CRC KEY (START = 13579246)
3	241	
132		
204		

15

20

25

After the first byte is keyed or encrypted, the CRC value for the next byte needs to be updated by taking the current CRC value and doing a Boolean EXCLUSIVE OR with the original byte. That value, in turn is Boolean ANDed with the hexadecimal number 255 which provides an index into the CRC table (between 0 and 255). The CRC table value that is looked up with that index is then Boolean EXCLUSIVE ORed with the CRC value shifted to the right 8 places, for example as shown below.

$$134579246 \wedge 3 = 13579245$$

$$13579245 \& 255 = 237$$

$$\text{CRC_TABLE}[237] = 3736837829$$

$$13579246 \gg 8 = 53043$$

3736837829 \wedge 53043 = 3736818166, which is now the new CRC value as illustrated in TABLE 3:

30

TABLE 3

ORIGINAL DATA FILE	NEW DATA FILE	CRC KEY (START = 13579246)
1	3	3736818166
132		
204		

The process is repeated for each byte in the file, for example as shown in TABLE 4 below.

TABLE 4

BYTE NUMBER	ORIGINAL DATA FILE	NEW DATA FILE	CRC KEY (START = 13579246)
1	3	241	3736818166
2	132	122	3201674049
3	204	13	2478254646

The process is repeated for each byte in the file.

In order to decode or decrypt the data bytes, the process is simply reversed starting with the same known seed CRC key and the same base CRC table values, for example as illustrated in TABLE 5 below.

TABLE 5

BYTE NUMBER	KEY DATA FILE	NEW DATA FILE	CRC KEY (START = 13579246)
1	241		
2	122		
3	13		

Initially, the first byte from the keyed file is read, for example 241. The current value of the CRC key (13579246) is subtracted from that value. The result (-13579005) is Boolean ANDed with 255 which provides a result of 3 which was the original starting point for example as shown in TABLE 6 below.

TABLE 6

BYTE NUMBER	KEY DATA FILE	NEW DATA FILE	CRC KEY (START = 1359246)
1	241	3	
2	122		

BYTE NUMBER	KEY DATA FILE	NEW DATA FILE	CRC KEY (START = 1359246)
3	13		

The CRC key is then updated for the next byte. In order to update the CRC key essentially the same 5 method is used as before. The new byte 3 is EXCLUSIVE ORed with the current value of the CRC key (13579246). The result (13579245) is then Boolean ANDed with the 10 hexadecimal number 255 with a result of 237 which is used as an index to look the CRC value in the CRC lookup table. The current example of the index corresponds to 15 a table value of 3736837829. The current CRC key (13579246) is then shifted to the right 8 places. The result 53043 is EXCLUSIVE ORed with the value that was looked up in the CRC table (3736837829) by way of the index 237. The result 3736818166 is the CRC for the new byte, for example as shown in TABLE 7 below.

TABLE 7

BYTE NUMBER	KEY DATA FILE	NEW DATA FILE	CRC KEY (START = 13579246)
1	241	3	3736818166
2	122		
3	13		

For the next byte the current CRC key 25 3736818166 is subtracted from the next byte read 122, the result being 558149252. This result 558149252 is anded with the hexadecimal number 255 to produce the next byte 132 which, is the original byte number in the original data file. The process is repeated for each byte as shown below in TABLE 8.

TABLE 8

BYTE NUMBER	KEY DATA FILE	NEW DATA FILE	CRC KEY (START = 13579246)
1	241	3	3736818166
2	122	132	3201674049
3	13	204	2478254646

The process is repeated until the end of the file and the end result is that the output file exactly corresponds to the original file which was encrypted.

Obviously, many modifications and variations of the present invention are possible in light of the above teachings. Thus, it is to be understood that, within the scope of the appended claims, the invention may be practiced otherwise than as specifically described above.

What is claimed and desired to be secured by Letters Patent of the United States is: